SANDIA NATIONAL LABORATORIES

Discover Awards

Data Encryption Standard Application Specific Integrated Circuit

Nomination ID: 129

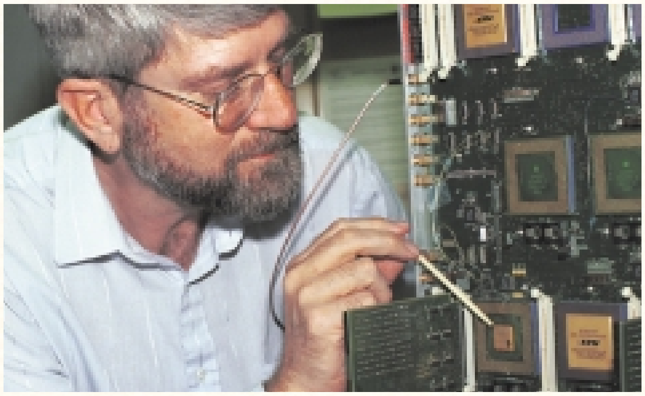
Sandia National Laboratories

A Department of Energy National Laboratory

Data Encryption Integrated Circuit

Award category:
Communications

Name of innovation:
Data Encryption Standard Application Specific Integrated Circuit (unclassified encryptor chip)



Lyndon Pierson points to the unclassified encryptor chip – the world's fastest encryption device – that his Sandia research team designed.

Describe the innovation in a few sentences.
The world's fastest encryption device, developed at the Department of Energy's Sandia National Laboratories, protects data as it is being transmitted between supercomputers, workstations, telephones, and video terminals. It encrypts data at more than 6.7 billion bits per second, 10 times faster than any other known encryptor. At the same time, it offers both the security and bandwidth necessary to protect all types of digitized information—voice, audio, video, cell phone conversations, radio and television transmissions, banking and credit card information, and general-purpose computer data—at speeds previously unimagined. While the device has been tested at encryption speeds of 6.7 billion bits per second, it actually can operate much faster. Simulations predict that it can operate at 9.28 billion bits per second.

How does the innovation work?
The device uses the Data Encryption Standard algorithm, a mathematical transformation commonly used to protect data by cryptographic means. The encryptor consists of 16 sets of 16,000 transistors on an integrated circuit chip the size of a dime. Data, broken down into single bits of information in 64-bit units, is pipelined through the transistors, where the computationally intense algorithm scrambles the information so it becomes incomprehensible without the cryptographic key.

The 16 sets of transistors are key to the speed of the new encryption device. Other devices typically have one set of approximately 16,000 transistors that cycle data bits 16 times in order to encrypt it. The new device pipelines information bits in clocked cycles through the 16 sets of transistors. This pipelining increases the device's speed by dividing the algorithm into 16 equally sized blocks, maximizing operational frequency.

This approach also allows the encryptor to process data differently on each clock cycle. For example, the device may encrypt data with one mathematical key on one clock cycle, decrypt new data with a different key on the next clock cycle, bypass the algorithm and not encrypt the data on the following clock, and then encrypt data with another independent key on the fourth clock cycle, resulting in a high degree of agility not found in any other encryptor/ decryptor.

What problem did this innovation solve?
Fast encryption and decryption are particularly important when sending or receiving large amounts of secure data via telephone wires, fiber optics, or satellites. The next-fastest commercial encryptor operates at 0.6 billion bits per second, resulting in long waits while large amounts of data move from one communication source to another. The new system is the first encryption device fast enough to secure the standard 2.5 Gb/s and 10 Gb/s communication channels now being used to carry the ever-increasing streams of data for Internet commerce. The device can also be cost-effectively manufactured on a large scale to satisfy these high-speed communication requirements.

Why is it important?
This technology addresses the already burgeoning demand for increased communication speed and data protection. The need to protect sensitive data will only increase as Internet-based trade continues to expand.

How will this innovation benefit the average consumer or the public in general?
Consumers benefit by protecting confidential medical, financial, or proprietary business data and preventing it from falling into the hands of computer hackers, thiefs, or corporate spies. The device is suitable for use on high-end or personal computers.

When was this innovation developed, released or launched?
A news release publicized this accomplishment on July 5, 1999.

Is any information about this innovation available on the Web?
If so, please give us the URL:
http://www.sandia.gov/media/NewsRel/NR1999/encrypt.htm

Data Encryption Integrated Circuit

Who came up with this innovation (list all)?
Lyndon Pierson
Byron Dean
Karl Gass
Perry Robertson
Tom Tarman
Edward Witzke
Craig Wilcox

Of these people, who is the person MOST responsible for its development? We realize that most innovations are the work of a team of people, but we require the name of the ONE researcher, scientist or engineer most responsible.) If selected as a finalist, the ONE person here will be featured in Discover and invited to attend the awards ceremony.
Name: Lyndon Pierson
Title: Senior Scientist
Company: Sandia National Laboratories
Address: P.O. Box 5800, MS 0806, Albuquerque, NM 87185-0806
Phone: (505) 845-8212
Fax: (505) 844-2067
Email: lgpiers@sandia.gov

Whom should we contact if we need more explicit information about the innovation?
Lyndon Pierson

Name of person completing this form:
Noel Fletcher, Linda Doran, Lyndon Pierson

How did you hear about the Discover Awards:
Previous award winners.

Are you a subscriber to the magazine:
No.

SUPPORTING MATERIALS

MAGAZINE AND NEWSPAPER ARTICLES:
"Did You Know That…," News and Trends, *Security Management*, October 1999.

Hankins, Michelle L., "Integrated Circuit Chip Provides Secure, Rapid Data Encryption," Security, *Signal*, October 1999, pp. 47–48.

"Sandia Researchers Develop World's Fastest Encryptor," *Sandia Technology*, Fall 1999, p. 7.

Gavacs, Jenny, "High-Speed Encryptor Developed," Information Management, *R&D Magazine*, September 1999, p. 13.

"The Fastest Encryptor in the East, West, North, and South, Too," Technology Bulletin, *Design News*, Aug. 16, 1999, p. 16.

"High-Speed Encryption," *Aviation Week & Space Technology*, Aug. 9, 1999.

"This Is One Speedy Encryptor," Breaking News, *Government Computer News*, Aug. 2, 1999.

"Sandia Researchers Develop World's Fastest Encryptor: Soon Will Protect Classified Computer Information," News Release, Sandia National Laboratories, July 5, 1999.

Burroughs, Chris, "Sandia Researchers Develop World's Fastest Encryptor: Device Encrypts Data at More Than 6.7 Billion Bits Per Second," *Sandia Lab News*, June 18, 1999.

TECHNICAL DATA:
Summary information and photographs contained in technical paper, Sandia National Laboratories, August 1999.

"DES ASIC Data Sheet," preliminary data presented by Sandia National Laboratories, Sept. 4, 1998.

TECHNICAL REPORT:
Wilcox, D.C., Pierson, L.G., Robertson, P.J., Witzke, E.L., and Gass, K., "A DES ASIC Suitable for Network Encryption at 10 Gbps and Beyond," proceedings in *Cryptographic Hardware and Embedded Systems, First International Workshop*, (Worcester, Mass.,) Aug. 12-13, 1999.